БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

ФИО преподавателя: Селин А.А., канд. техн. наук

УРОВНИ ЗАЩИТЫ ДАННЫХ В СОВРЕМЕННЫХ СУБД

Учебные вопросы:

1. Составляющие безопасности баз данных
2. Виды идентификации пользователя в базе данных
3. Перспективные технологии защиты баз данных

СОСТАВЛЯЮЩИЕ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Безопасность базы данных = **ЗАЩИТА ПОДКЛЮЧЕНИЙ** + **АУДИТ ДЕЙСТВИЙ** + **ЗАЩИТА ДАННЫХ**

Каждое подключение – потенциальный канал утечки данных!

Субъект обработки данных – это пользователь или прикладная программа.

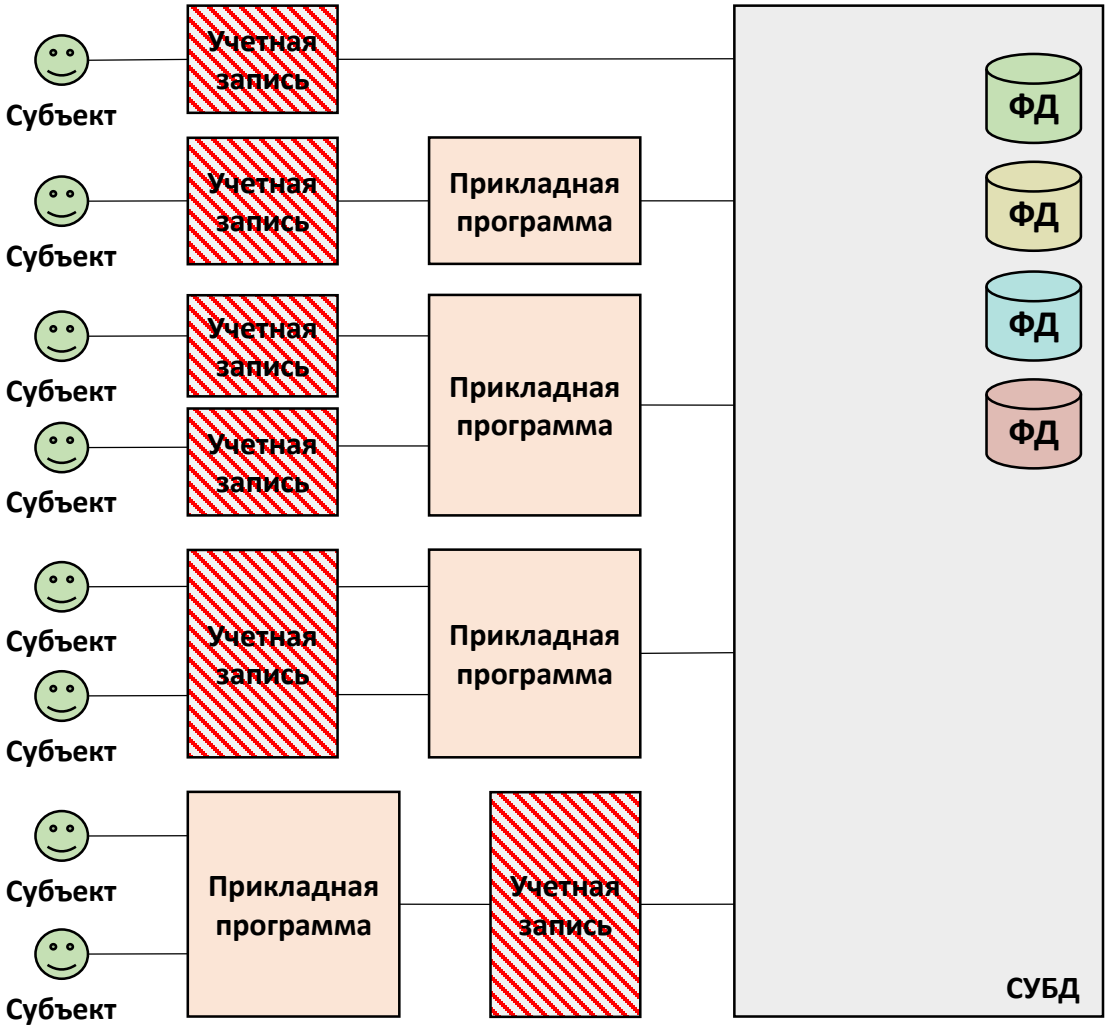
Каждая учетная запись должна быть надежно аутентифицирована.

Никакой субъект не должен иметь возможность прямого редактирования данных в таблице.

Никакие промежуточные слои (pooling/proxy/middleware) не должны иметь возможность влиять на параметры подключения.

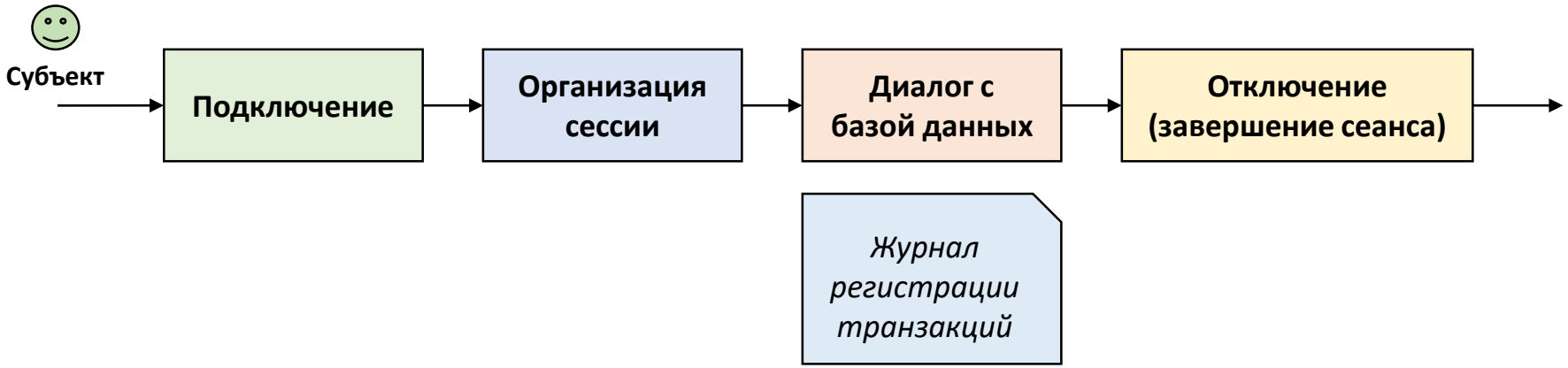
По возможности необходимо обеспечить, чтобы один бизнес-пользователь соответствовал одному пользователю базы данных.

Каждое подключение порождает документируемую сессию.



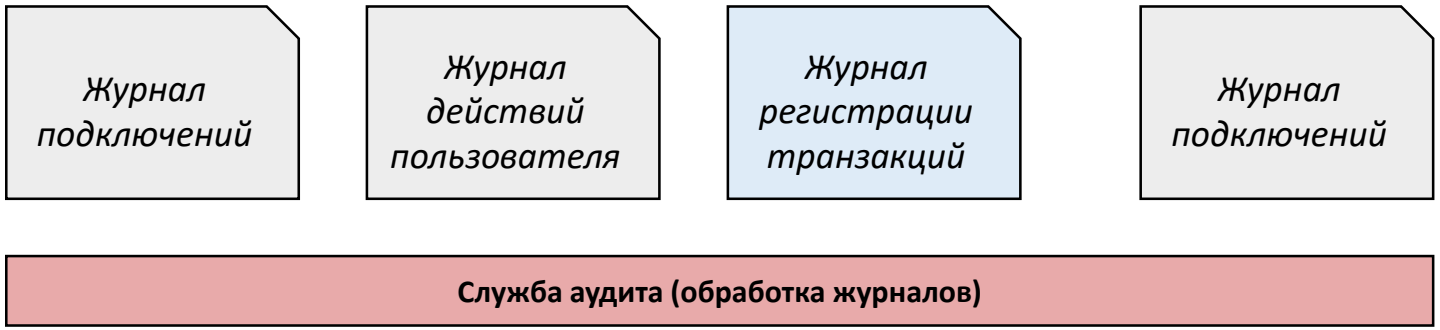
СОСТАВЛЯЮЩИЕ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Безопасность базы данных = **ЗАЩИТА ПОДКЛЮЧЕНИЙ** + **АУДИТ ДЕЙСТВИЙ** + **ЗАЩИТА ДАННЫХ**

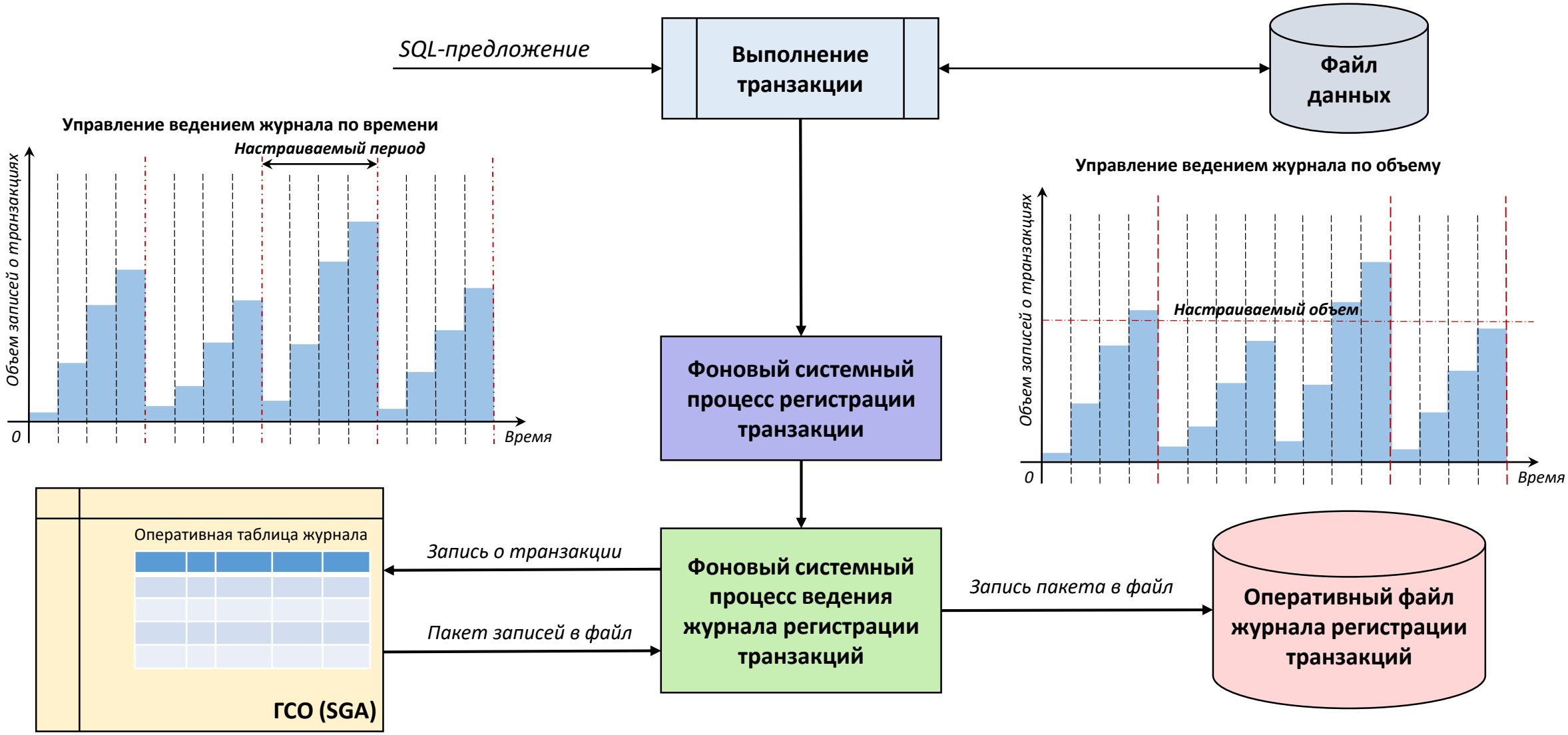


Open Source: PostgreSQL, MySQL, SQLite,…

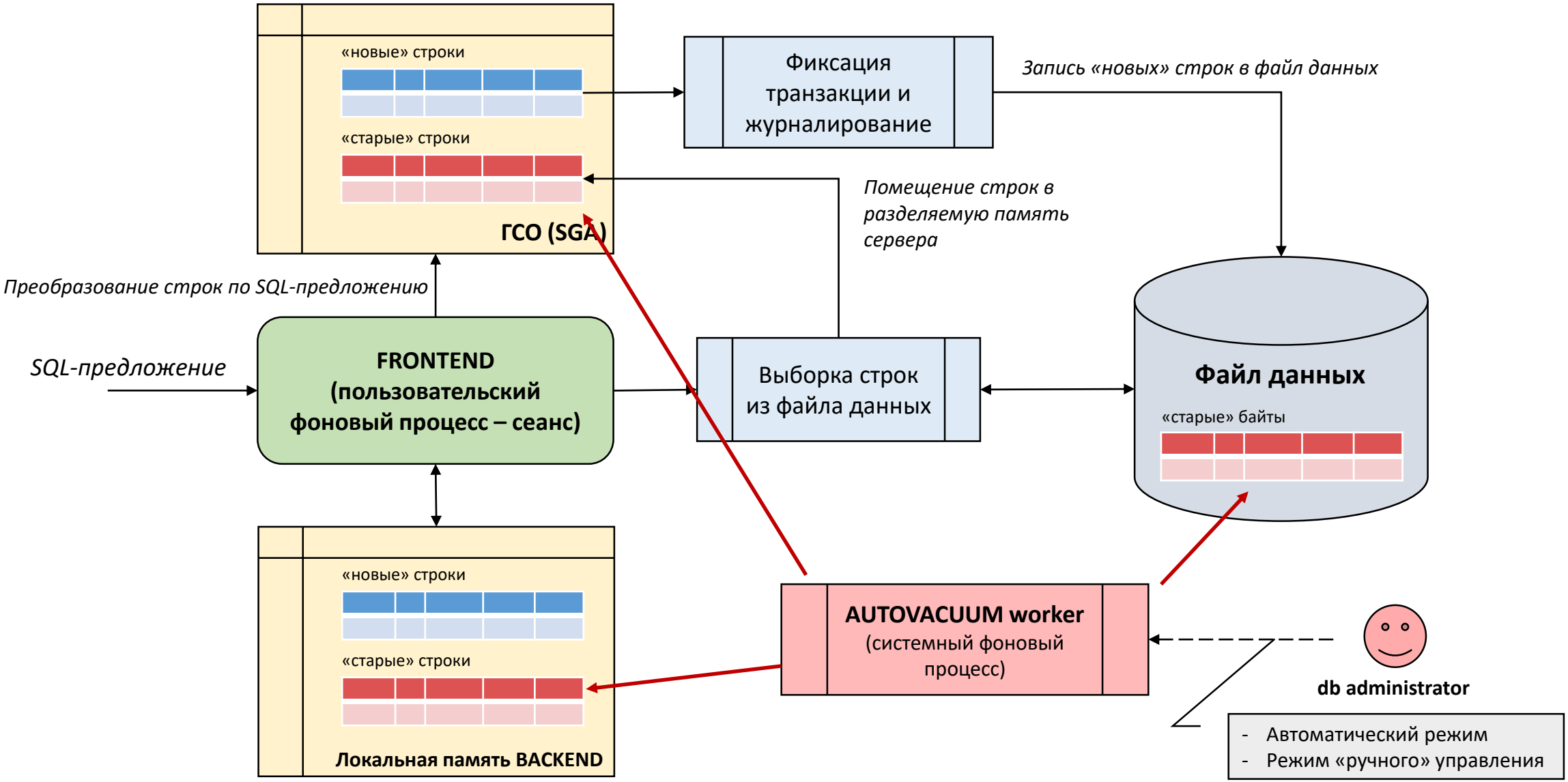
Enterprise: Oracle, SQL Server, Ingres,…



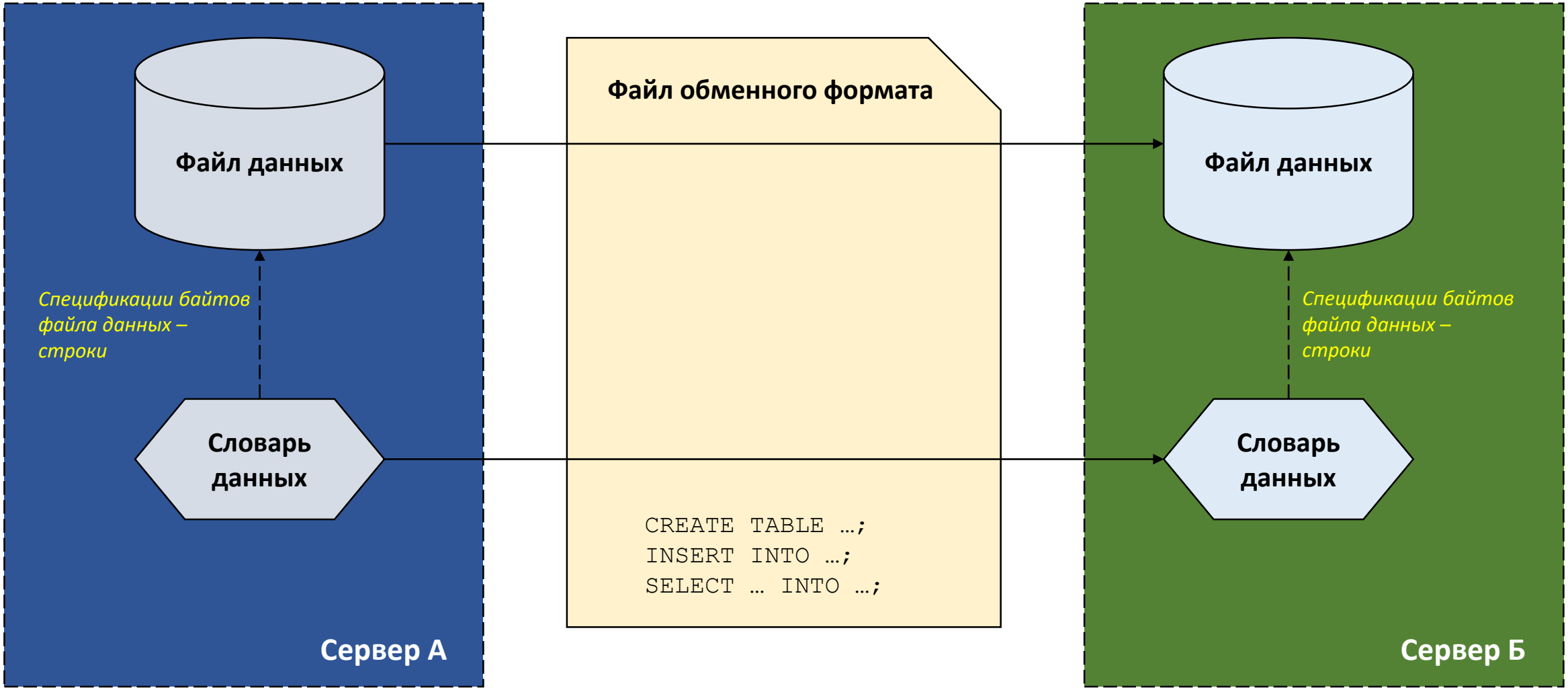
СОСТАВЛЯЮЩИЕ БЕЗОПАСНОСТИ БАЗ ДАННЫХ



СОСТАВЛЯЮЩИЕ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

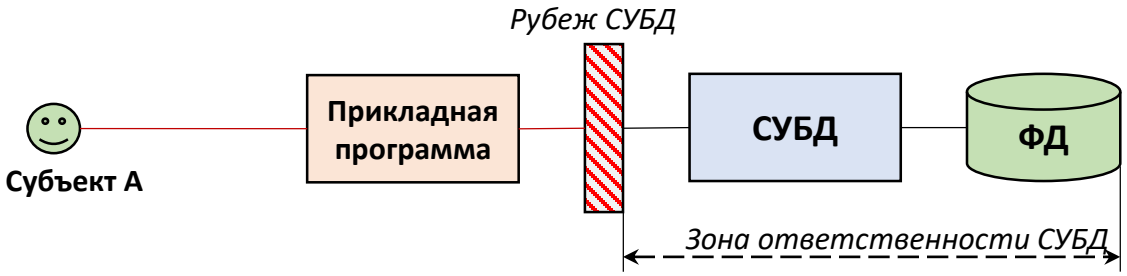


СОСТАВЛЯЮЩИЕ БЕЗОПАСНОСТИ БАЗ ДАННЫХ



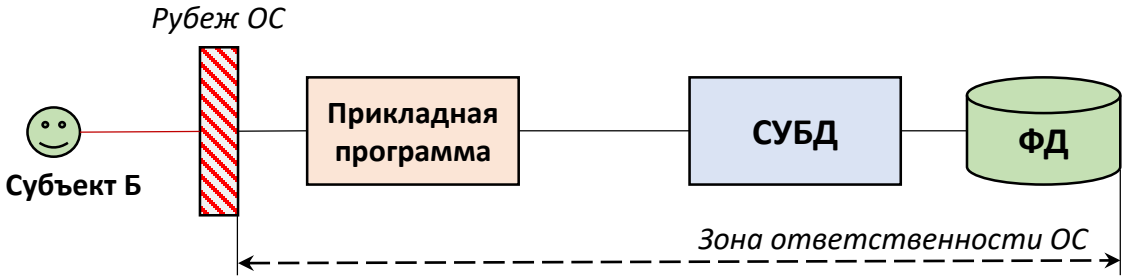
ВИДЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В БАЗЕ ДАННЫХ

Идентификация в базе данных




```
<Имя_учетной_записи>/<Пароль>@<Имя_экземпляра>

SQL> Connect User_01/P_02aRy4@instant_6
```

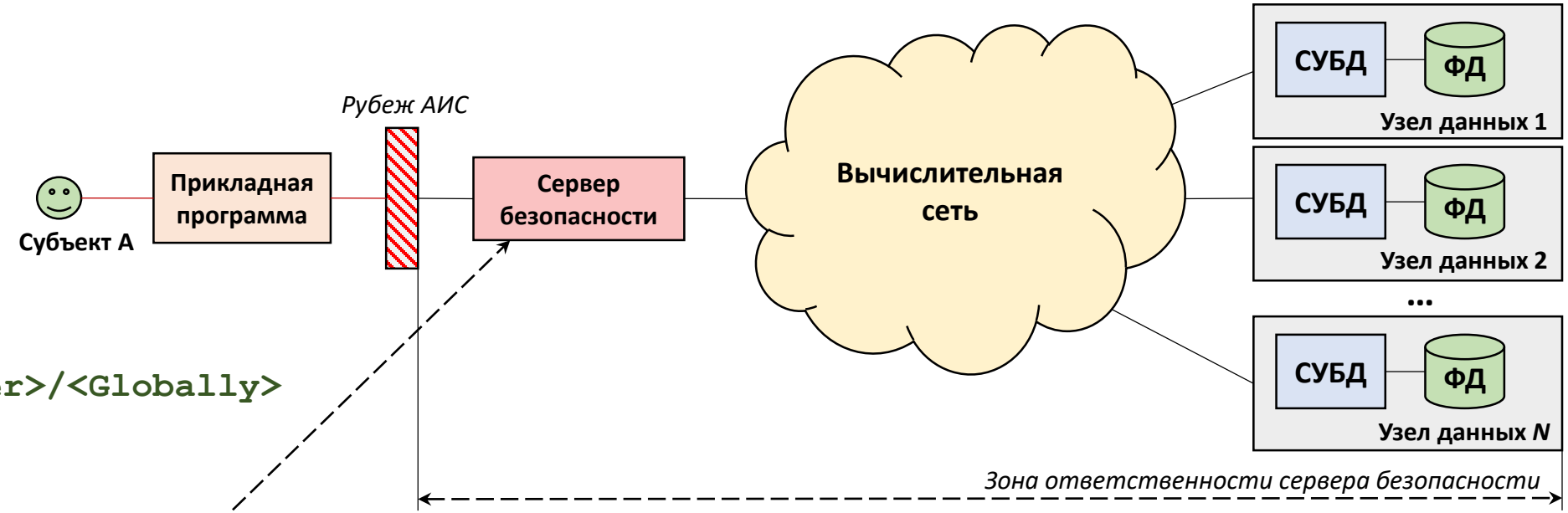
Внешняя идентификация




```
OS AUTHENT PREFIX = <Префикс>

<Префикс><Имя_учетной_записи>

OS AUTHENT PREFIX = DBU$

DBU$User_01  – будет допущен к сервисам БД
User_01      – не будет допущен к сервисам БД
```

ВИДЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В БАЗЕ ДАННЫХ

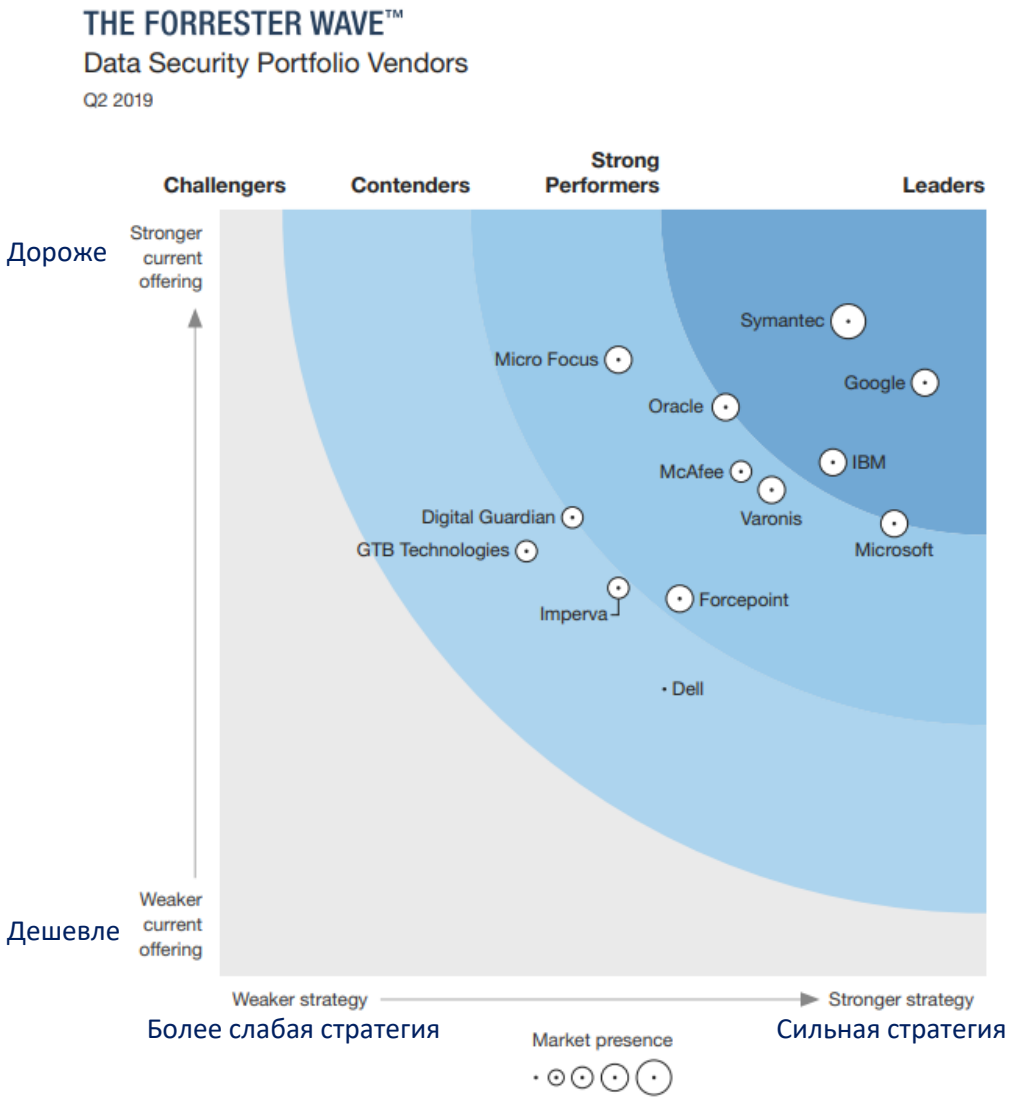
Идентификация на уровне предприятия



Data Activity Monitoring (DAM) – система мониторинга действий пользователей: аутентификация пользователей;
распределение полномочий;
анализ транзакций пользователей;
выявление потенциально опасной активности;
оценка защищенности сервисов БД

DataBase Firewall (DBF) – сетевой экран базы данных: фильтрация телетрафика в портах системы баз данных;
шифрование данных обмена в структуре базы данных;
анализ информационных потоков через порты системы баз данных;
выявление потенциально опасных потоков данных

ВИДЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В БАЗЕ ДАННЫХ

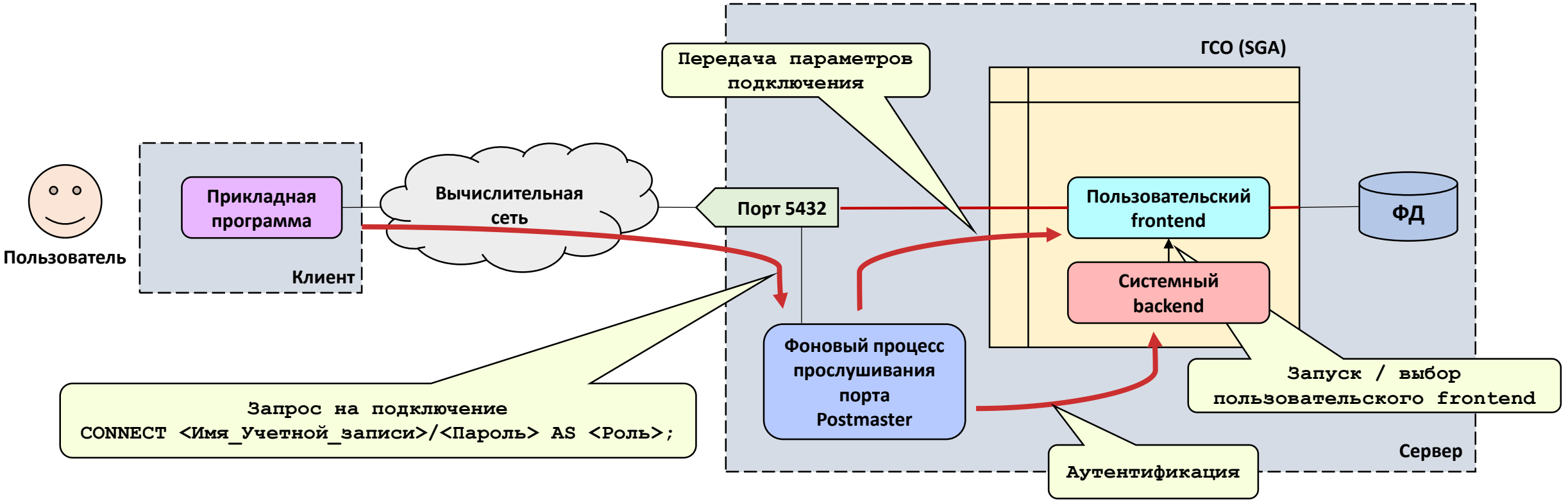


Российские комплексы и системы защиты баз данных

	МФИСофт Гарда БД	Аладдин Крипто БД	SearchInform Database Monitor (DM)	СБЕР Platform V Pangolin	PP Postgres Pro Enterprise
Класс	**DAM**	**DBF**	**DAM**	**Embedded**	**Embedded**
Мониторинг потоков данных	+	+	+	-	-
Контроль обращений к данным (FGAC – тщательный контроль доступа)	+	-	+	+	+
Активная защита	+	+	+	+	-
Сканирование на уязвимости	+	+	-	-	-
Шифрование файлов данных (TDE)	+	+	-	+	+

ВИДЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В БАЗЕ ДАННЫХ

Процедура подключения к базе данных



Режим сервера баз данных: **DEDICATED** – каждому сеансу пользователя назначается (запускается) собственный backend
SHARED – сеанс пользователя обслуживает любой свободный backend

ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ БАЗ ДАННЫХ

Технологии хранения и обработки данных

BIG DATA – хранение и обработка данных, отличающихся следующими свойствами:

Volume – значительный объем (свыше миллиона строк или более 1 терабайта данных)

Velocity – быстродействие обработки данных значительного объема (методы поиска и преобразования)

Variety – высокая разнообразность данных (по типам: смешанные типы, не стандартные типы, преобразование типов)

in memory – хранение и обработка оперативных данных в энергозависимой памяти вычислительной системы (мобильные данные, оперативные данные с коротким жизненным циклом, данные управления по телеметрии,..)

NoSQL (not only SQL, NoRDBMS, NoRelational) – попытка решить проблемы масштабируемости и доступности за счёт полного или частичного отказа от требований атомарности и согласованности данных. В отличие от реляционных СУБД (транзакционная модель с совокупностью свойств **ACID**) опирается на совокупность свойств **BASE**:

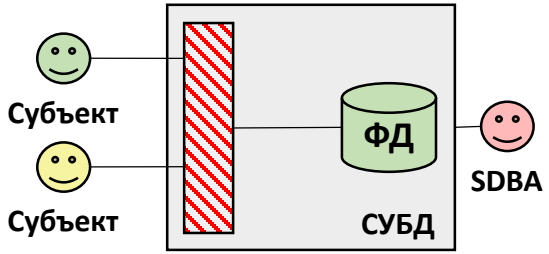
базовая доступность (англ. **BA**sic availability) – каждый запрос гарантированно завершается (успешно или безуспешно),

гибкое состояние (англ. **S**oft state) – состояние системы может изменяться со временем, даже без ввода новых данных, для достижения согласования данных,

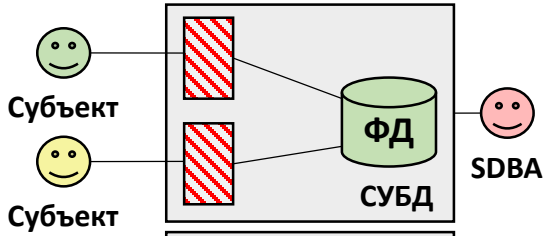
согласованность в конечном счёте (англ. **E**ventual consistency) – данные могут быть некоторое время рассогласованы, но приходят к согласованию через некоторое время).

HTAP – гибридная транзакционная (OLTP) / аналитическая (OLAP) обработка данных

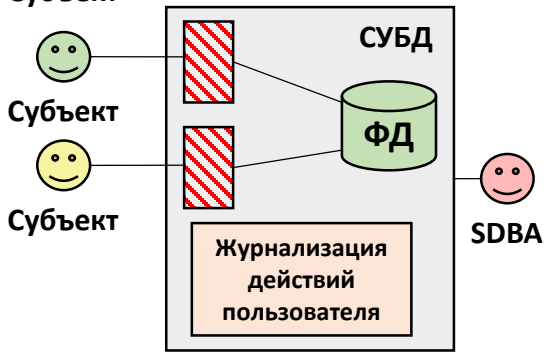
ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ БАЗ ДАННЫХ



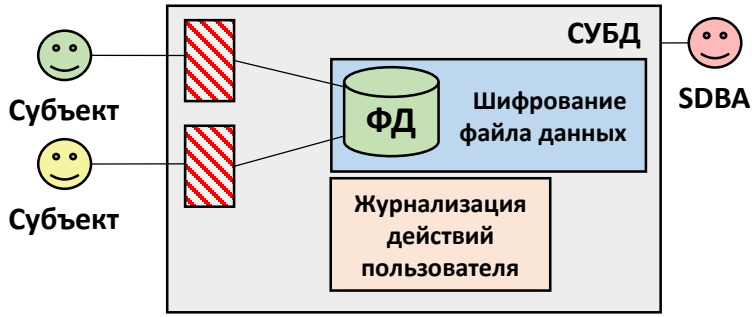
1. Организация идентификации и аутентификации пользователей – создание «барьера» информационной безопасности.



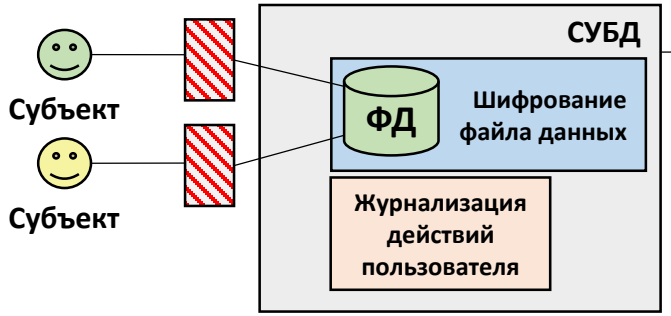
2. Разграничение пользователей в соответствии с их уровнями благонадежности – дискреционный доступ.



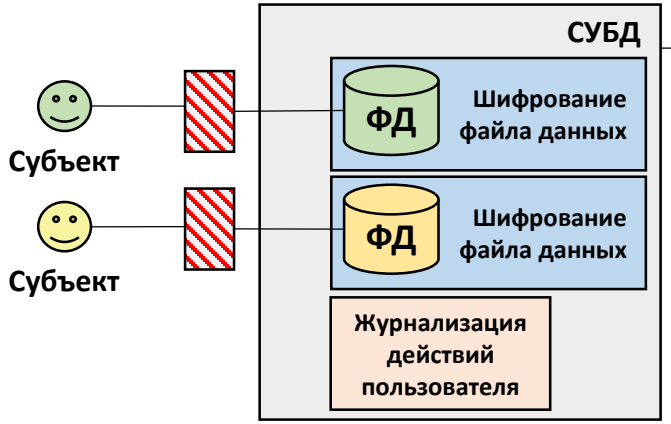
3. Введение журнализации действий пользователей и аудита информационной безопасности.



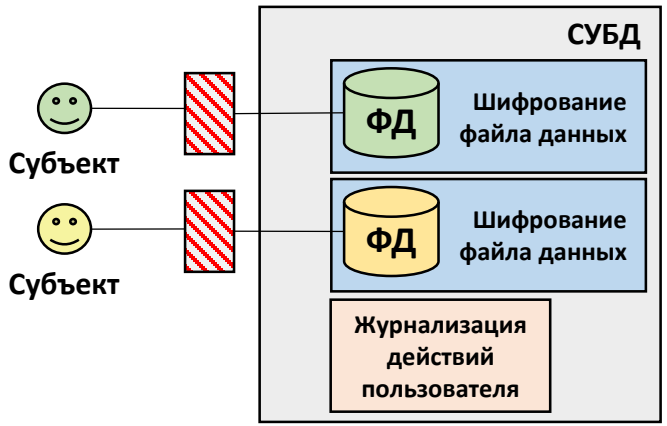
4. Шифрование файлов данных.



5. Вынос аутентификации из СУБД в операционную систему – применение выделенных программных средств обеспечения информационной безопасности.



6. Разграничение (изоляция) данных с разными степенями конфиденциальности, создание надежного компонента переднего плана.

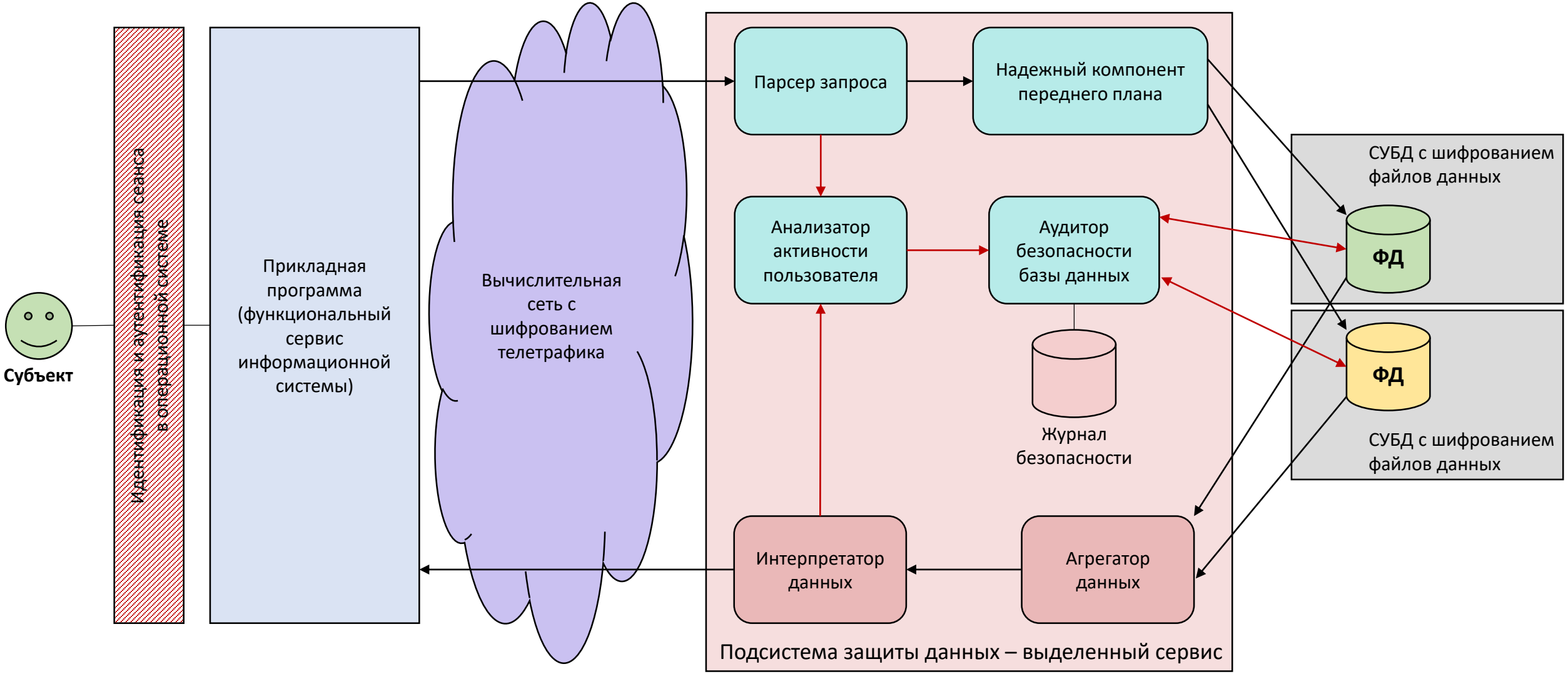


7. Отказ от доверенного администратора безопасности

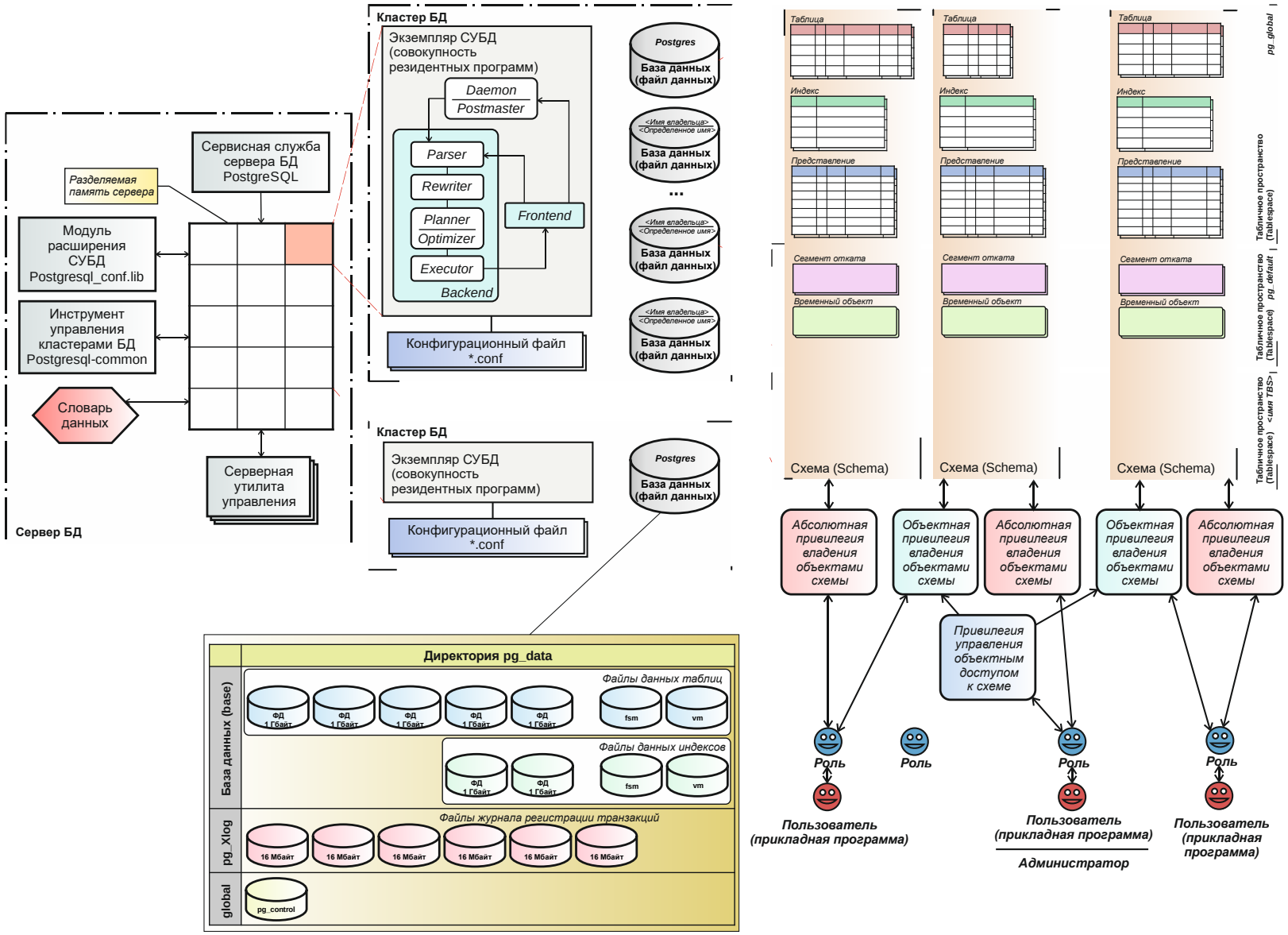
RoadMap архитектуры безопасной базы данных

ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ БАЗ ДАННЫХ

Обобщенная архитектура безопасной системы баз данных



ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ БАЗ ДАННЫХ



СУБД PostgresPro = PostgreSQL + подсистема защиты

PostgresPro Enterprise
PostgresPro Standart

Сертификат ФСТЭК России № 4063 от 21.04.2022 г.

Единый реестр российских программ для электронных вычислительных машин и баз данных запись № 104 от 18.03.2016 г.

Компания-разработчик:
Postgres Professional HQ
117312, г. Москва, ул. Дмитрия Ульянова, 7А

Литература:

1. **Смирнов, С. Н.** Безопасность систем баз данных [Текст]: учеб. пособие для вузов по специальностям в области информационной безопасности. – М.: Гелиос АРВ , 2007. – 350 с.

2. **Федин, Ф. О.** Информационная безопасность баз данных. Ч. 1 [Электронный ресурс]: учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — М.: РТУ МИРЭА, 2020. — Электрон. опт. диск (ISO)

3. **Саймон, А. Р.** Стратегические технологии баз данных: менеджмент на 2000 год: Пер. с англ. /Под ред. и с предисл. М. Р. Когаловского. - М.: Финансы и статистика, 1999 - 479 с.: ил.

4. **Терьо, М.** Oracle. Руководство по безопасности [Текст] / М. Терьо, А. Ньюмен; Пер. с англ.. — М.: Лори, 2004. — 560 с.: ил.

5. **Кузнецов, С. Д.** Основы баз данных: курс лекций : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. ин-форм. технологий / С. Д. Кузнецов. – Москва: Интернет-ун-т ин-форм. технологий, 2005. – 488 с.

6. **Смирнов, С. Н., Задворьев, И. С.** Работаем с ORACLE.: Учебное пособие/2-е изд., испр. и доп. – М: Гелиос АРВ, 2002 г. – 496 с.

7. **Кульба, В.В.** и др. Теоретические основы проектирования оптимальных структур распределенных баз данных. – М: СИНТЕГ, 1999 г. – 660 с.

8. Материалы сервера ORACLE/RE. www.oracle.ru/press/magazine/main.html

9. Материалы информационного ресурса WIKIPEDIA. https://ru.wikipedia.org/wiki/Разграничение_доступа_на_основе_атрибутов; https://ru.wikipedia.org/wiki/Аутентификация; https://ru.wikipedia.org/wiki/Многофакторная_аутентификация; https://ru.wikipedia.org/wiki/Сложность_пароля.

10. Материалы информационного ресурса http://www.nsc.ru/ws/YM2003/6299/